STATE OF ALABAMA

Information Technology Standard

Standard 630-03S1: E-Mail Usage

1. INTRODUCTION:

State of Alabama affords broad access to information technology resources for State employees to use for business purposes, serving the interests of the government and of the people it serves in the course of normal operations. The appropriate use of State email and email distribution lists must meet certain standards to ensure the integrity and availability of e-mail system resources.

2. OBJECTIVE:

Define requirements for and prohibited uses of State of Alabama e-mail systems.

3. SCOPE:

These requirements apply to all users (State employees, contractors, vendors, and business partners) of any State of Alabama e-mail systems.

4. REQUIREMENTS:

All electronic communications are expected to comply with relevant Federal and State laws, as well as State policies and standards, including those governing information technology resources and security considerations.

4.1 PROHIBITED USES OF STATE E-MAIL

The following activities are prohibited:

- Sending or forwarding remarks and/or images considered obscene, offensive, racist, libelous, slanderous, or defamatory
- Using a State email account to send or forward virus or malware warnings, security advisories, terrorist alerts, or other mass-mailings without prior approval of the agency IT Manager, Information Security Officer, or Group Distribution List Owner unless in the course of normal assigned duties
- Sending unsolicited email messages including junk mail, spam, or other advertising material to individuals who did not specifically request such material except in the execution of normal government information dissemination
- Postings to newsgroups by personnel using a State email address unless in the course of business duties
- Using State email for personal or commercial ventures, religious or political causes, endorsement of candidates, or supporting non-government organizations
- Sending or forwarding chain letters or joke emails

- Disguising or attempting to disguise your identity when sending email
- Sending email messages using another person’s email account
- Intercepting email messages destined for others
- Unauthorized use, forging, or attempting to forge email header information or messages

4.2 AUTO-FORWARDING STATE E-MAIL

To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding shall not be used to send State e-mail to an Internet address.

4.3 MASS E-MAIL

Material sent to group distribution lists must be relevant to the group being mailed and shall pertain to State business and/or serve the interests of State employees or constituents.

4.3.1 Message Content/Format

Message format may be text, HTML, or RTF and should not include attachments.

HTML or RTF format messages may contain artwork, but shall be limited to a single page.

Each message shall contain a signature block with the sender’s name, departmental affiliation, office telephone number, and email address.

Sender is responsible for all replies, responses, and complaints.

4.3.2 Message Approval

It is the responsibility of the sender/requestor of a mass e-mail to obtain the necessary approval from the person, group, or designated owner of the distribution list.

Authority to use the “all-employees” distribution list rests with the Governor’s office.

Approval authority for agency/organization-level groups (e.g., “ISD – All Users”) shall rest with the manager or management team presiding over that group.

Message shall include a line indicating the State office that approved the mass e-mail.

4.3.3 Message Transmission

Mass electronic mailings shall only be transmitted in the evenings (after 5pm).

4.3.4 List Owner Responsibilities

Owners of group distribution lists shall develop and monitor compliance with written operating procedures for the use of their lists. All list owners are encouraged to consider the benefits of moderating or otherwise controlling access to large lists. This applies whether a list has been created for one-time use or is maintained as a standing list.

5. DEFINITIONS:

MALWARE: Short for malicious software (such as a virus or Trojan horse); software designed specifically to damage or disrupt a system.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 630-03: E-Mail Usage

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/7/2006	